

REMARKS/ARGUMENTS

Characteristics of IBE

In identifier-based encryption (IBE), the data to be encrypted (the first data set of claim 1) is encrypted using as encryption parameters:

- public data of a trusted third party – in the present case, this is preferably the public point $R(=sP)$ as described at page 10, line 21 of the present application where s is a secret (private data) of the trusted authority;
- a public key string Q_{ID} (see page 10, line 23) – in the present case, this string is preferably a printing policy Q_{print} (see page 11, line 8)

The key S_{ID} for decrypting the encrypted data is generated by the trusted third party using:

- the public key string;
- private data of the third party, in this case the secret s .

In the present case, S_{ID} (also called S_{print}) is generated as sQ_{ID} (see page 10, line 26)

Generation of the decryption key can be effected at any time and does not have to be done at the same time as generation of the public key string Q_{ID} . The role of the trusted party is to ensure that any conditions in the public key string (in this case, printing policy conditions) have been complied with before the decryption key is supplied for use (in the preferred embodiment, to the printer).

Using the public data of the trusted party as an encryption parameter ensures that only the trusted party can generate the private key needed for decryption.

Clarity Issue

Claim 1 as originally filed recited:

“ - a first computing entity arranged to encrypt a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium, the first computing entity being further arranged to output the encrypted first data set for the output device; and” (emphasis added)

The examiner has apparently taken the word “comprising” to refer to the first data set rather than to the encryption parameters as was intended (see the Examiner’s comment near the end of page 3 of the Official Action). In order to avoid any possible ambiguity here the above passage is amended by this response to read as follows:

“a first computing entity arranged to encrypt a first data set based on encryption parameters that comprise:

public data of a trusted party, and

an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium,

the first computing entity being further arranged to output the encrypted first data set for the output device; and”

Similar amendments have been effected to claims 15 and 28.

Claims 39 and 40

Claims 39 and 40 are cancelled without prejudice.

The Schneck Reference (US 6,314,409)

The Examiner has rejected all the claims as allegedly being fully anticipated by the Schneck reference.

Schneck discloses the distribution of data of interest in encrypted form as packaged data 108. The data of interest is encrypted using a symmetric encryption algorithm and key K_D . This key K_D is encrypted using a key K_R and included in the packaged data. The key K_R is called the rule-encrypting key and is also used to encrypt rules governing use of the data of interest. These rules may be included in the packaged data 108 in encrypted form (encrypted using K_R) or may be provided to the user separately of the packaged data. Perhaps K_R , in one context, is really the public key of an asymmetric key pair, the private key of which (also called by the very same term K_R in Schneck) is known only to a user's computer (presumably protected within the tamper-resistant access mechanism 114) – see col. 12, lines 26-28 and col. 14, lines 43-61 of Schneck.

Difference between Claim 1 and Schneck

Claim 1 requires the encryption of data using, as encryption parameters, public data of the trusted party and an encryption key string formed by the output policy. Clearly Schneck does not use his rules as an encryption parameter for encrypting anything.

Regarding the “public data” of the trusted party, one might assert that the key K_R of Schneck, might form the public data of a trusted party (this is based on assuming that K_R is the public key of an asymmetric key pair); in this case, the “first data set” of claim 1 would need to be understood as being either the key K_D or the rules of Schneck, as these are apparently the only elements of Schneck for which K_R constitutes an encryption parameter. In either case, this interpretation of the “first data set” does not fit with other parts of claim 1

Claim 1 also requires that the decryption key be generated by “second computing entity associated with the trusted party” after satisfying itself that the “policy has been met”. The entity in Schneck that checks the rules appears to be the accessing entity 114 and the entity is not described as generating any key.

Furthermore, according to claim 1, the decryption key is generated in dependence on the encryption key string and private data related to said public data. There is no equivalent disclosure in Schneck. The passages referred to by the examiner on page 4, line 14 of the Official Action do not disclose how any decryption key is generated by the second computing entity as required by claim 1.

Similar arguments apply to independent claims 15 and 28.

Schneck is not a proper prior art reference

Schneck does not appear to be an enabling document. Note the discussion of Figure 4. At step S404 Schneck teaches that the data-encrypting key is itself encrypted with the rule-encrypting key K_R and that this encryption is carried out by the authoring mechanism 112 of distributor 102. See column 12, lines 29-38 of Schneck. But Schneck also specifically teaches that the rule-encrypting key K_R “is known only to (and protected within) each receiving computer of each user.” See column 12, lines 27-29 of Schneck.

So exactly how is the distributor 102 supposed to use an encrypting key known only to the user’s computer? Schneck contemplates public key schemes - note the reference to asymmetric encryption algorithms at column 12, line 14. But those skilled in the art realize that asymmetric encryption algorithms have public and private keys.

It seems that perhaps Schneck uses the symbols, such as K_R , to refer rather indiscriminately to both public and private keys. Which is which in the

Schneck disclosure? And why is an apparent private key K_D being itself encrypted and then delivered to a third party? How is a person of ordinary skilled supposed to make heads or tails of this disclosure? Perhaps the author did not have a good understanding of cryptography fundamentals.

If the Examiner intends on relying on Schneck in any future official actions, the Examiner is respectfully requested to explain in detail whether any keys referred to in Schneck are a private or public key and whether they are being used for encryption or decryption and how a person of ordinary skill would so understand Schneck. Any factual assertions need to be placed into affidavit format as required by 37 CFR 1.104(d)(2).

The IDS

The Examiner objected to the IDS filed with this application. It is believed that the objections raised by the Examiner are, with all due respect, without merit. For example, the Examiner asserts that the IDS contains a "different inventor than in the oath of declaration submitted with this application". That assertion is not correct as both identify "Cheh Goh" and others. The Examiner also asserts that the IDS contains "the wrong attorney docket number". That assertion is also not correct as both identify the attorney docket number as "B-5236 621255-8".

The undersigned telephoned the Examiner about this point and was informed that the real issue was that the IDS did not identify the application by application number. Well since no application number was assigned as of the date this application was expressed mailed to the USPTO, the applicants and/or their attorney would had to have been clairvoyant to have guessed the application number in advance. There is no need to identify an IDS filed with a new application with a then unknown and unassigned application number.

Kindly withdraw the objection to the originally filed IDS as having been made improvidently.

If the Examiner is unwilling to withdraw the objection to originally filed IDS, then an interview with both the Supervising Examiner who signed the Official Action and the Group Director prior to the issuance of another official action is respectfully requested.

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2125.

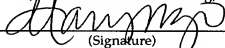
I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

April 13, 2007

(Date of Transmission)

Mary Ngo

(Name of Person Transmitting)

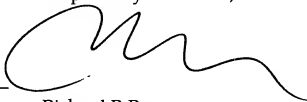


(Signature)

April 13, 2007

(Date)

Respectfully submitted,



Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile